USMEPCOM PRIVACY IMPACT ASSESSMENT (PIA)

1. **Department of Defense Component:**
United States Military Entrance Processing Command (USMEPCOM)

2. **Name of Information Technology System:**
USMEPCOM Integrated Resource System (USMIRS)

3. **Budget System Identification Number (SNAP-IT Initiative Number):**
1191

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):**
81

5. **IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):**
007-21-01-20-01-1191-00-201-067

6. **Privacy Act System of Records Notice Identifier:**
A0601-270 USMEPCOM DoD.

7. **OMB Information Collection Requirement Number and Expiration Date:**
N/A – USMIRS is a legacy system that existed prior to requirement.

8. **Type of authority to collect information (statutory or otherwise):**

a. E.O. 9397 (SSN)

b. 10 U.S.C. 3013, Secretary of the Army

c. 10 U.S.C. 8013, Secretary of the Air Force

d. 10 U.S.C. 5013, Secretary of the Navy

e. DoD Directive 1145.2E, "United States Military Entrance Processing Command (USMEPCOM)," dated January 8, 2005

f. DoD Directive 1304.12, "DoD Military Personnel Accession Testing Programs," dated June 22, 1993

g. DoD Directive 1304.26, "Qualification Standards for Enlistment, Appointment and Induction," dated December 21, 1993 (Will add to notice)

h. DoD Instruction 4000.19, "Interservice and Intragovernmental Support," dated August 9, 1995

i. DoD Directive 6130.3, "Physical Standards for Appointment, Enlistment, and Induction," dated December15, 2000

j. Army Regulation 601-270/Air Force Regulation 33-7/Marine Corps Order P1100.75A, Military Entrance Processing Station (MEPS)

k. USMEPCOM Regulation 680-3, U.S. Military Processing Command Integrated Resources System (USMIRS)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):

The mission of USMEPCOM is to ensure applicants entering into the Military Service meet the Service qualification standards. To collect required applicant qualification information, USMEPCOM personnel administer aptitude tests, medical examinations, initiate background-screening checks and process enlisted contracts. These qualification services are provided at 65 military entrance processing stations (MEPSs) located throughout the United States and Puerto Rico. The automation USMEPCOM currently uses to collect applicant qualification information is the USMEPCOM Integrated Resource System (USMIRS).

The USMIRS Data Center is located at Headquarters, USMEPCOM, 2834 Green Bay Road, North Chicago, IL 60064. Customers include:

- Applicants for enlisted military service
- United States Army Recruiting Command (USAREC)
- United States Navy Recruiting Command
- United States Marine Corps Recruiting Command
- United States Air Force Recruiting Command
- United States Coast Guard Recruiting Command
- United States Army Training and Doctrine Command (TRADOC)
- Defense Manpower Data Center (DMDC)
- Office of Personnel Management (OPM)
- Office of the Secretary of Defense, Manpower

a. **Information Collection.** USMIRS collects daily enlisted accession data and provides reporting capability to USMEPCOM, DMDC, Office of the Secretary of Defense and to approved military accession community organizations.

b. **Record Retention**. Each MEPS retains a copy of reporting system source documents for each enlistee for 90 days after shipment. For all other applicants, each station retains, if applicable, a copy of the Report of Medical Examination (DD Form 2808) with supporting documentation, the Report of Medical History (DD Form 2807), and any other reporting source documents, for a period not to exceed 2 years unless the applicant failed to meet minimum medical enlistment standards which are kept for 7 years, after which they are destroyed. Originals or copies of documents are filed permanently in Official Personnel Files for acceptable applicants and transferred to the gaining Armed Forces Component. Test

score transmittals and qualification test answer records are maintained for one year and then destroyed. Test material inventory files are maintained until inventory is approved and destroyed when no longer needed for conducting business, but not kept for more than 6 years.

c. **Information Sharing**. Formal interface agreements are developed for all organizations with which USMEPCOM shares its data. This list includes stakeholders (listed below) and customers. Within these agreements is a requirement for a certified and accredited network infrastructure before an electronic interface is established. The primary vehicle for this electronic data sharing is the certified and accredited Recruiting Services Network operated and maintained by USAREC. USMIRS, a legacy system, is being replaced by the Virtual Interactive Processing System (VIPS). USMIRS is projected to end its current function and configuration by FY-13. It will be retired as VIPS begins to ramp up and becomes implemented.

Stakeholders include:

- Department of Homeland Security
- Air Force Reserve Command (AFRC)
- Air Force Recruiting Information Support System (AFRISS)
- Army Recruiting Information Support System (ARISS)
- Army Research Institute (ARI)
- Army Reserve National Guard (ARNG)
- United States Army Recruiting Command (USAREC)
- United States Army Accessions Command (USAAC)
- United States Army Cadet Command (USACC)
- United States Army Training and Doctrine Command (TRADOC)
- United States Army Deputy Chief of Staff for Personnel (G-1)
- Army Medical Surveillance Activity (AMSA) - USACHPPM
- United States Coast Guard Recruiting Command
- Defense Finance and Accounting Service (DFAS)
- Defense Integrated Military Human Resource System (DIMHRS)
- Defense Manpower Data Center (DMDC)
- Defense Security Service (DSS)
- Office of Personnel Management (OPM)
- Selective Service System (SSS)
- Surface Deployment and Distribution Command (SDDC)
- United States Citizenship and Immigration Services (USCIS)
- Marine Corps Recruiting Information Support System (MCRISS)
- Marine Corps Recruiting Command (USMCRC)
- Naval Education and Training, Professional Development and Technology Center (NETPDTC)
- Navy Drug Screening Lab (NDSL)

- Navy Recruiting Accession Management System (NRAMS)
- Space and Naval Warfare - Information Technology Center (SPAWAR-ITC)
- US Navy Recruiting Command (NRC)
- Military Surface Deployment and Distribution Command (SDDC)
- U.S. Army Medical Command (MEDCOM)
- Accession Policy (AP), Military Personnel Policy (MPP), Personnel and Readiness (P&R)
- Department of Defense Medical Examination Review Board (DoDMERB)
- Office of the Surgeon General (OTSG)
- National Civilian Community Corps (NCCC)

10. **Identifiable Information to be Collected, its Nature and Source**
The recruit identification number is the primary identifier (index key) of records. The social security number is the secondary index key identifier. The database includes the following primary personal information: individual's name, social security or alien registration number, date and place of birth, home address and telephone number, ethnicity, aptitude tests results , physical examination results along with medical information, background screening results through use of fingerprinting and criminal history.

11. Method of Information Collection:

Personal information is provided by individuals and Service recruiters. USMIRS information is collected using a paper-based collection via forms and electronic documents generated in Microsoft Office product suite formats and and Jetform forms software. Information is entered directly from Service recruiters and liaisons via electronic systems.

12. Purpose of Collection:

To establish eligibility for enlistment, verify enlistment and placement scores, verify retest eligibility, and provide aptitude test scores as an element of career guidance to participants in the Department of Defense (DoD) Student Testing Program. The data is also used for research, marketing evaluation, assessment of manpower trends and characteristics, and related statistical studies and reports.

13. How Identifiable Information/Data will be Used:

USMEPCOM is currently the only DoD organization legally authorized to collect civilian, medical and testing data for purposes of processing enlistment applicants into the military. USMIRS is the only DoD joint support system in operation that is used to enforce congressional, DoD, and Armed Forces qualification criteria for enlistment. It is used as an official system for reporting timely enlistment accession data to DMDC. Information collected is also disclosed to the Selective Service System (SSS) to update its registrant database and may also be disclosed to local and state Government agencies for compliance with laws and regulations governing control of communicable diseases.

14. Does system create new data about individuals through aggregation?

Yes.

15. Internal and External Information/Data Sharing:

Internal to USMEPCOM: Data will be shared among ASVAB testing personnel, medical personnel, legal staff, recruiting and career counselor personnel, and various Headquarters and MEPS personnel who have a need to access.

External to USMEPCOM: US Citizenship and Immigration Services, Surface Deployment and Distribution Command, Army Research Institute, Defense Finance and Accounting Service, OPM, Joint Advertising Market Research and Studies, Joint Accessions Research (JAR), Naval Education and Training Professional Development and Technology Center, Defense Accession Data Systems Integration Working Group (DADSIWG) members, Navy Drug Screening Lab, United States Army Accessions Command, SSS, TRADOC, DMDC, military training bases, reception stations, Military Treatment Facilities at the training bases, Accessions Medical Standards and Research Analysis (AMSARA), and local and state Government agencies.

16. Opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted:

Personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement.

17. Information Provided to the Individual, the Format, and the Means of Delivery:

When requested in writing, information is provided to individuals in accordance with the guidance prescribed in Army Regulation 340-21 (The Army Privacy Program). Electronic formats will be made available upon request and availability. Information is delivered by regular mail (normally FedEx 2-Day service), e-mail, or fax.

18. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

The USMIRS users include Active Duty Military and Federal Civil Service personnel at USMEPCOM and at each of the individual MEPS. Both contractor and government employees may have access requirements to specific or general information in the USMIRS computing environment. The System Administrator (SA) is required to define the specific access requirements for each user's role. Each specific application may further restrict access via application-unique permission controls. All personnel accessing government computer information are required to undergo at the minimum a National Agency Check.

Currently, only USMEPCOM users and service liaisons (and their authorized contract users) have the capability to connect to the USMIRS system. With the exception of Systems Administrators, Information Assurance Security Officers (IASOs), and software maintenance personnel, USMIRS users fall into non-sensitive Information Technology (IT)

Category III (non-privileged) positions as designated in DoD Directive 8500.1. Persons in IT Category-III positions require a National Agency Check, Entrance National Agency Check, or National Agency Check with Inquiries. All SA, IASOs, and software maintenance personnel are in non-sensitive IT Category-I (privileged) positions. Persons in IT Category-I positions require a Single Scope Background Investigation (SSBI). Information is made available to USMEPCOM users through the USMIRS application, Enterprise server or QuICR. Each authorized user must enter an appropriate User/Identification and Password before being authorized access to the resources.

There is weekly monitoring and immediate disabling of accounts with easily guessed passwords, daily notification of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). USMEPCOM accession partners are provided information through regularly scheduled file transfers accomplished via ftp or email across the RSN or Non-classified but Sensitive Internet

Protocol Router Network (NIPRNET). Files transferred across the Internet/NIPRNET are encrypted using a Virtual Private Network (VPN) or Advanced Encryption Standard (AES) 256-bit encryption.

19. Privacy Act Interface: System of Records notice published Feb 25, 2005 at http://www.dod.mil/privacy/notices/army

20. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures:
Appropriate safeguards are in place for the collection, use, and sharing of information. Individuals who object to providing required information may be unable to enter the Armed Forces. Security measures are adequate and risk is minimal. Information is protected by user passwords, firewalls, antivirus software, CAC access, and data-at-rest protection software on portable laptops.

21. Classification and Publication of Privacy Impact Assessment:
The Privacy Impact Assessment may be published in its entirety.